UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/754,813	01/04/2001	Jing Min Xu	JP919990266US1	3476

48813 7590 03/09/2007

LAW OFFICE OF IDO TUCHMAN (YOR)
82-70 BEVERLY ROAD
KEW GARDENS, NY 11415

EXAMINER	
WONG, LESLIE	
ART UNIT	**PAPER NUMBER**
2164	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
2 MONTHS	03/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/754,813
Filing Date: January 04, 2001
Appellant(s): XU ET AL.

Ido Tuchman
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 31 October 2005 appealing from the Office action mailed 31 May 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,442,689	Kocher	08-2002
6,128,740	Curry et al.	10-2000
6,411,956	Ng	06-2002
6,658,568	Ginter et al.	12-2003
6,304,882	Strellis et al.	10-2001

Vesna Hassler, "X.500 and LDAP security: a comparative overview", Network, IEEE, Vol. 13, Issue 6, (Nov.-Dec. 1999), pp. 54-64

Kaliski, B. "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and rrelated Services", RFC 1424, (Feb. 1993), pp. 1-8

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 4, 6, 7, 10, 11, 13-15, and 17-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (6,442,689) in view of Curry et al. ("Curry", 6,128,740) and further in view of Ng (6,411,956).

As per claim 1, Kocher teaches a system comprising:

a plurality of certificate authorities (CAs) in which each CA maintains and distributes digital certificates revoked by itself in the form of a certificate revocation list (CRL), and different CAs may use different CRL distribution mechanisms (Kocher, col. 2, lines 17-31, col. 3, lines 15-18);

a plurality of CRL databases for storing the consolidated CRLs from multiple CRL retrieval agents and/or the replications of CRLs, the CRL databases storing at least one individually identifiable revoked digital certificate (Kocher, col. 3, lines 15-18).

Kocher does not explicitly disclose multiple CRL retrieval agents configured to periodically retrieve CRLs at time intervals from different CAs using a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs. Curry discloses multiple CRL retrieval agents configured to periodically retrieve CRLs at time intervals from different CAs using a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs (col. 2, lines 26-41; col. 5, lines 23-27, 34-43; col. 6, lines 33-38). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the CRL system of Kocher by incorporating the means of using multiple CRL retrieval agents to periodically retrieve CRLs as disclosed by Curry (Curry, col. 2, lines 26-41). The motivation being to determine whether the digital certificate is valid, thereby ensuring the integrity of the system.

Neither Kocher nor Curry discloses a CRL access user interface for providing a uniform set of Application Program Interfaces for users accessing the CRLs in the CRL database. Ng teaches an access user interface for providing a uniform set of APIs for users accessing the database (Ng, col. 1, lines 15-18). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Kocher and Curry's combined system by incorporating a uniform set of APIs as disclosed by Ng (col. 1, lines 15-18). The motivation being to provide easy access to the CRLs using a single interface.

As per claim 4, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, and further disclose said plurality of CRL retrieval agents include a HTTP/CRL retrieval agent, for periodically retrieving CRLs from specified HTTP servers and updating the CRL database (Kocher, col. 1, line 19 - col. 2, line 67).

As per claim 6, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, and further disclose said plurality of CRL retrieval agents include a HTTP retrieval agent triggered by a HTTP request, said HTTP receiver agent verifies an authorization of the requester, if successful, said agent stores each transmitted CRL in the CRL databases (Kocher, col. 3, line 1 - col. 4, line 56, col. 10, lines 64-67).

As per claim 7, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, and further disclose said plurality of CRL retrieval agents further verifies the integrity and the authenticity of the retrieved CRLs (Kocher, col. 3, line 1 - col. 4, line 56).

As per claim 10, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, and further disclose said system is also adapted for consolidating and accessing at least one kind of revoked certificate list (Kocher, col. 3, line 1 - col. 4, line 56).

As per claim 11, Kocher teaches in a secure network implemented by digital certificates, a method for certificate revocation list (CRL) consolidation and access, wherein a plurality of certificate authorities (CAs) maintain and distribute the digital certificates revoked by themselves in the form of CRLs, and different CAs may use different CRL distribution mechanisms, said method comprising the steps of:

creating a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs, for consolidating the CRLs from multiple CAs (Kocher, col. 2, line 17 - col. 3, line 18);

storing the consolidated CRLs from multiple CRL retrieval agents or the replications of CRLs into a plurality of CRL databases, the consolidated CRLs including at least one individually identifiable revoked digital certificate (Kocher, col. 2, line 17 - col. 3, line 18).

Kocher does not explicitly disclose periodically retrieve CRLs at time intervals from different CAs using a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs. Curry discloses periodically retrieve CRLs at time intervals from different CAs using a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs (Curry, col. 2, lines 26-41). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to

modify the CRL system of Kocher by incorporating periodically retrieving CRLs using a plurality of CRL retrieval agents as disclosed by Curry (Curry, col. 2, lines 26-41). The motivation being to determine whether the digital certificate is valid, thereby ensuring the integrity of the system.

Neither Kocher nor Curry discloses accessing the CRLs from the CRL databases by a uniform set of Application Program Interfaces. Ng teaches an access user interface for providing a uniform set of APIs for users accessing the database (Ng, col. 1, lines 15-18). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Kocher and Curry's combined system by incorporating a uniform set of APIs as disclosed by Ng (col. 1, lines 15-18). The motivation being to provide easy access to the CRLs using a single interface.

As per claim 13, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 11, and further disclose said method is also adapted for consolidation and accessing all kinds of black lists (Kocher, col. 3, line 1 - col. 4, line 56).

As per claim 14, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 11, and further disclose an article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 11 (Kocher, col. 1, line 1 - col. 4, line 56).

As per claim 15, Kocher, Curry and Ng g teach all the claimed subject matters as discussed in claim 11, and further disclose a computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing certificate revocation list (CRL) consolidation and access, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 11 (Kocher, col. 1, line 1 - col. 4, line 56).

As per claim 17, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 11, and further disclose a program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for certificate revocation list (CRL) consolidation and access, said method steps comprising the steps of claim 11 (Kocher, col. 1, line 1 - col. 4, line 56).

Claim 18 is rejected on grounds corresponding to the reasons given above for claim 11.

Claim 19 is rejected on grounds corresponding to the reasons given above for claim 17.

Claim 20 is rejected on grounds corresponding to the reasons given above for claim 14.

Claim 21 is rejected on grounds corresponding to the reasons given above for claim 15.

3. Claims 2, 8 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (6,442,689) in view of Curry et al. ("Curry", 6,128,740) in view of Ng (6,411,956) and further in view of Ginter et al. ("Ginter", 6,658,568).

As per claim 2, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, and further teach a central CRL database (Kocher, col. 2, lines 17-31, col. 3, lines 15-18). Kocher does not explicitly disclose a plurality of CRL replication databases storing the replications of the CRLs of the central CRL database. Ginter discloses a plurality of CRL replication databases storing the replications of the CRLs of the central CRL database (Ginter, col. 80, line 56, col. 81, lines 19-24). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Kocher, Curry and Ng's combined system by incorporating a plurality of CRL replication databases as disclosed by Ginter (col. 80, line 56, col. 81, lines 19-24). The motivation being to reduce the workload at the central CRL database and divide the workload among the plurality of CRL replica databases. This will improve the processing speed.

As per claim 8, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, except for explicitly disclosing a particular replication architecture is used among said plurality of CRL databases in order to maintain database consistency. Ginter discloses a particular replication architecture is used among said plurality of CRL databases in order to maintain database consistency (Ginter, col. 80, line 56, col. 81, lines 19-24). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Kocher, Curry and Ng's

combined system by incorporating a replication architecture as disclosed by Ginter (col. 80, line 56, col. 81, lines 19-24). The motivation being to produce a plurality of CRL replica databases, and divide the workload among the plurality of CRL replica databases. This will improve the processing speed.

Claim 12 is rejected on grounds corresponding to the reasons given above for claim 2.

4. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (6,442,689) in view of Curry et al. ("Curry", 6,128,740) in view of Ng (6,411,956) and further in view of Vesna Hassler ("Hassler", "X.500 and LDAP security: a comparative overview", Network, IEEE, Volume: 13 Issue: 6, Nov.-Dec. 1999, Page(s): 54-64).

As per claim 3, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, except for explicitly disclosing said plurality of CRL retrieval agents include a LDAP/CRL retrieval agent, for periodically retrieving CRLs from specified LDAP servers and updating the CRL databases. Hassler discloses said plurality of CRL retrieval agents include a LDAP/CRL retrieval agent, for periodically retrieving CRLs from specified LDAP servers and updating the CRL databases (Hassler, page 54). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Kocher, Curry and Ng's combined system by incorporating a LDAP/CRL retrieval agent as disclosed by Hassler (page 54). The motivation being to provide an agent to retrieve and verify the digital certificate in LDAP system.

5. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (6,442,689) in view of Curry et al. ("Curry", 6,128,740) in view of Ng (6,411,956) and further in view of Kaliski, B; ("Kaliski", "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services", RFC 1424, Feb. 1993, pp. 1-8).

As per claim 5, Kocher, Curry and Ng teach all the claimed subject matters as discussed in claim 1, except for explicitly disclosing said plurality of CRL retrieval agents include a RFC1424/CRL retrieval agents, for periodically sending RFC1424/CRL retrieval request and receiving CRL retrieval reply. Kaliski discloses said plurality of CRL retrieval agents include a RFC1424/CRL retrieval agents, for periodically sending RFC1424/CRL retrieval request and receiving CRL retrieval reply (Kaliski, page 1). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Kocher, Curry, Ng's combined system by incorporating RFC1424/CRL retrieval agent as disclosed by Kaliski (page 1). The motivation being to provide an agent to retrieve and verify the digital certificate in Internet Electronic Mail system.

6. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher (6,442,689) in view of Curry et al. ("Curry", 6,128,740) in view of Ng (6,411,956) in view of Ginter et al. ("Ginter", 6,658,568) and further in view of Strellis et al. ("Strellis", 6,304,882).

As per claim 9, Kocher, Curry, Ng and Ginter teach all the claimed subject matters as discussed in claim 2, except for explicitly disclosing a hub-and-spoke replication architecture is used among said central CRL database and said plurality of

CRL replication databases. Strellis discloses disclosing a hub-and-spoke replication architecture is used among said central CRL database and said plurality of CR.L replication databases (Strellis, col. 10, lines 14-21). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Kocher, Curry, Ng and Ginter's combined system by incorporating a hub-and-spoke replication architecture as disclosed by Strellis (col. 10, lines 14-21). The motivation being to maintain the consistency between the central database and plurality of replica databases.

(10) Response to Argument

Arguments (1): Appellant argues that there is no teaching of multiple CRL retrieval agents configured to periodically retrieve CRLs at time intervals from different CAs using a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs as recited in claim 1.

In response to the preceding arguments, Examiner respectfully submits that Curry teaches the limitation "multiple CRL retrieval agents configured to periodically retrieve CRLs at time intervals from different CAs using a plurality of CRL retrieval agents based on the CRL distribution mechanisms of CAs" as utilizing certification **authorities or managers** (i.e., multiple retrieval agents) that collect revoked certificates and queue them to publish them on a periodic basis with other existing revoked certificates (col. 2, lines 37-41). Further, Curry teaches if a security officer or software application (i.e., different CAs) must revoke a certificate because a user of the client has

left the company or if a private key has been compromised, the security officer may activate a GUI interface button indicating that a certificate revocation request has been activated. If on-demand publishing is not requested, the on-demand publish/queue determinator 34 queues the stored revocation serial number 36 in revocation database 38 for the *next preset automatic CRL update* (i.e., periodically retrieve) as show in block 64 (col.5, lines 23-27, lines 34-43). Additionally, Curry teaches if the CRL caching has been activated, meaning that the client or network node (i.e., CRL retrieval agents based on the CRL distribution mechanisms) periodically accesses the CRL repository 16 to get a current certificate revocation list and then stores the data locally, the network node 14 searches the CRL cache for the certificate revocation list as shown in block 92 (col. 6 lines 33-38). Hence, Curry teaches the limitation as claimed.

Appellant further argues that the examiner has not established a prima facie case of obvious of claim 1 and that obviousness cannot be established by combining prior art to produce the claimed invention absent some teaching or suggestion supporting the combination. In the present case, the advantage alleged by the Examiner to justify the proposed combination of Kocher and Curry does not stand up to close scrutiny. More particularly, the Examiner has not explained, and it is not evident, why a person of ordinary skill in the art would have found it obvious to reconstruct the Kocher system for creating digitally-signed lists to include the certificate revocation publishing methods taught by Curry. In this light, it is apparent the only suggestion for combining Kocher

and Curry in the manner advanced by the Examiner stems from hindsight knowledge impermissibly derived from the Appellant's disclosure.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

From MPEP § 2143.01[R-2] states:

"There are three possible sources for a motivation to combine references: the nature of the problem to be solved, the teachings of the prior art, and the knowledge of persons of ordinary skill in the art." *In re Rouffet*, 149 F.3d 1350, 1357, 47 USPQ2d 1453, 1457-58 (Fed. Cir. 1998) (The combination of the references taught every element of the claimed invention, however without a motivation to combine, a rejection based on a prima facie case of obvious was held improper.). The level of skill in the art cannot be relied upon to provide the suggestion to combine references. *Al-Site Corp. v. VSI Int'l Inc.*, 174 F.3d 1308, 50 USPQ2d 1161 (Fed. Cir. 1999).

"In determining the propriety of the Patent Office case for obviousness in the first instance, it is necessary to ascertain whether or not the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the reference before him to make the proposed substitution, combination, or other modification." *In re Linter*, 458

F.2d 1013, 1016, 173 USPQ 560, 562 (CCPA 1972).

Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either explicitly or implicitly in the references themselves or in the knowledge generally available to one of ordinary skill in the art. "The test for an implicit showing is what the combined teachings, knowledge of one of ordinary skill in the art, and the nature of the problem to be solved as a whole would have suggested to those of ordinary skill in the art." *In re Kotzab*, 217 F.3d 1365, 1370, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000). See also *In re Lee*, 277 F.3d 1338, 1342-44, 61 USPQ2d 1430, 1433-34 (Fed. Cir. 2002) (discussing the importance of relying on objective evidence and making specific factual findings with respect to the motivation to combine references); *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

In Ruiz v. A.B. Chance Co., 357 F.3d 1270, 69 USPQ2d 1686 (Fed. Cir. 2004), the patent claimed underpinning a slumping building foundation using a screw anchor attached to the foundation by a metal bracket. One prior art reference taught a screw anchor with a concrete bracket, and a second prior art reference disclosed a pier anchor with a metal bracket. The court found motivation to combine the references to arrive at the claimed invention in the "nature of the problem to be solved" because each reference was directed "to precisely the same problem of underpinning slumping foundations." Id. at 1276, 69 USPQ2d at 1690. The court also rejected the notion that "an express written motivation to combine must appear in prior art references...." Id. at 1276, 69 USPQ2d at 1690.

In this case, Appellant's invention is related to digital signature certificates and more particularly to certificate revocation lists consolidation and access. Kocher is directed to having a single trusted party collect digitally-signed lists (e.g., CRLs) from different trusted data item issuer (e.g., CAs) (abstract) and has specific application to revocation of digital certificates or other types of digital data items (col. 1, lines10-16). Curry is drawn to computer network security system provides generation of a certificate revocation list (CRL) upon each revocation. The entire certificate revocation list may be published on demand. The computer network security system stores the on-demand published data for analysis by one or more network nodes to determine whether a certificate is valid (col. 2, line 65 - col. 3, line 9). Both prior arts teach similar subject matters and are in the same field of endeavor of the claimed invention. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the CRL system of Kocher by incorporating the use of multiple CRL retrieval agents to periodically retrieve CRLs as disclosed by Curry to determine whether the digital certificate is valid (col. 3, line 9) in an effort to ensure the integrity of the system. As a result, it is submitted that combining Kocher and Curry to supplement the missing features that Kocher does not teach would have arrived at the invention as claimed.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Conclusion

Claims 1-15 and 17-21 are properly rejected under 35 U.S.C. 103(a).

In light of the foregoing arguments, the Examiner respectfully requests the Honorable Board of Appeals to sustain the rejections.

Respectfully submitted,

Leslie Wong
Primary Patent Examiner
Art Unit 2164

Conferees:

Don Wong
SPE Art Unit 2163

DON WONG
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Charles Rones
SPE Art Unit 2164

CHARLES RONES
SUPERVISORY PATENT EXAMINER